Cisco IOS ソフトウェアが稼動する Catalyst 6500/6000 での IEEE 802.1x 認証の設定例

内容

概要

このドキュメントでは、ネイティブ モード（スーパーバイザ エンジンと MSFC 用の単一の Cisco IOS® ソフトウェア イメージ）で稼働する Catalyst 6500/6000 および Remote Authentication Dial-In User Service（RADIUS）サーバ上で、認証および VLAN 割り当てのために IEEE 802.1x を設定する方法について説明します。

前提条件

要件

このドキュメントの読者は次のトピックについての専門知識を有している必要があります。

- Cisco Secure ACS for Windows 4.1 インストール ガイド
- Cisco Secure Access Control Server 4.1 ユーザ ガイド
- RADIUS はどのように動作しますか。
- Catalyst スイッチングおよび ACS 導入ガイド

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- スーパーバイザエンジンでCisco IOSソフトウェアリリース12.2(18)SXFが稼働するCatalyst 6500**注：**802.1xポートベース認証をサポートするには、Cisco IOSソフトウェアリリース12.1(13)E以降が必要です。
- この例では、RADIUS サーバとして Cisco Secure Access Control Server（ACS）4.1 を使用します。**注：スイッ**チで802.1xを有効にする前に、RADIUSサーバを指定する必要があります。
- 802.1x 認証をサポートする PC クライアント**注：この例**では、Microsoft Windows XPクライアントを使用しています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

IEEE 802.1x 標準では、認証されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、クライアントサーバ ベースのアクセス制御と認証プロトコルが定義されています。802.1x では、バーチャル アクセス ポイントを各ポートに 2 つ作成することで、ネットワーク アクセスが制御されます。片方のアクセス ポイントは制御されないポートであり、もう片方のアクセス ポイントは制御されたポートです。単一のポートを通過するすべてのトラフィックは、どちらのアクセス ポイントでも使用できます。802.1x では、スイッチ ポートに接続された各ユーザ デバイスが認証され、スイッチまたは LAN によって提供されるサービスが使用可能になる前にそのポートが VLAN に割り当てられます。802.1x アクセス制御では、デバイスが認証されるまで、そのデバイスが接続されているポートを通過する Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

注：スイッチが802.1x認証用に設定されていないポートからEAPOLパケットを受信した場合、またはスイッチが802.1x認証をサポートしていない場合、EAPOLパケットは廃棄され、アップストリームデバイスには転送されません。

設定

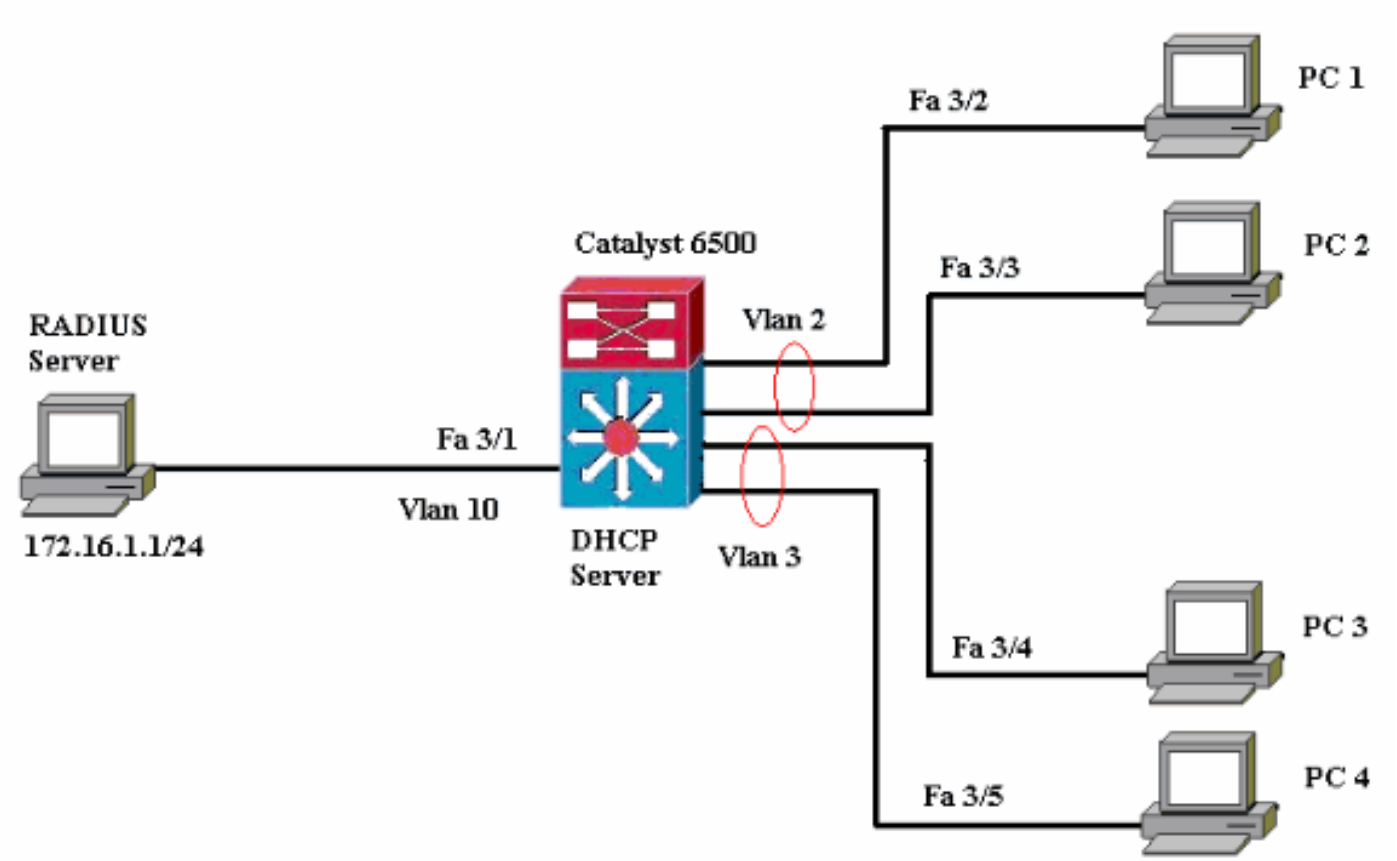
このセクションでは、このドキュメントで説明する 802.1x 機能を設定するための情報を提供します。

設定には次の手順が必要です。

- Catalystスイッチを802.1x認証用に設定します。
- RADIUS サーバを設定します。
- 802.1x 認証を使用するための PC クライアントの設定

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



- RADIUS サーバ：クライアントの実際の認証を実行します。RADIUS サーバは、クライアントの ID を検証し、クライアントが LAN およびスイッチ サービスにアクセスすることを承認されているかどうかをスイッチに通知します。ここで、RADIUS サーバの認証および VLAN 割り当ての設定が実行されます。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理的なアクセスを制御します。スイッチは、クライアントと RADIUS サーバ間の中継要素（プロキシ）として動作します。クライアントからの ID 情報を要求し、RADIUS サーバを使用してその情報を検証し、クライアントに応答を受け渡します。Catalyst 6500 スイッチは DHCP サーバとしても設定されます。802.1x 認証で Dynamic Host Configuration Protocol（DHCP）がサポートされているので、DHCP サーバは、認証済みユーザ ID を DHCP ディスカバリ プロセスに追加することにより、さまざまなクラスのエンド ユーザに IP アドレスを割り当てることができます。
- クライアント：LANおよびスイッチサービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ここで、1 ~ 4 の PC は、認証済みネットワーク アクセスを要求するクライアントです。PC 1と2はVLAN 2と同じログオン資格情報を使用します。同様に、PC 3と4はVLAN 3のログオン資格情報を使用します。PCクライアントは、DHCPサーバからIPアドレスを取得するように構成されています。

Catalyst スイッチでの 802.1x 認証の設定

このスイッチ設定のサンプルには次のものが含まれます。

- ファストイーサネットポートで802.1x認証を有効にする方法。

- ファストイーサネットポート3/1の背後にあるVLAN 10にRADIUSサーバを接続する方法。
- 2つのIPプール用のDHCPサーバ設定。1つはVLAN 2のクライアント用、もう1つはVLAN 3のクライアント用です。
- 認証後にクライアント間で接続を確立するためのインター VLAN ルーティング

802.1x認証の設定方法のガイドラインについては、『802.1xポートベース認証のガイドラインと制限事項』を参照してください。

注：RADIUSサーバが常に認可ポートの背後に接続していることを確認します。

Catalyst 6500

```
Router#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname Cat6K
!--- Sets the hostname for the switch.
Cat6K(config)#vlan 2
Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3
Cat6K(config-vlan)#name VLAN3
!--- VLAN should be existing in the switch for a
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER
!--- This is a dedicated VLAN for the RADIUS server.
Cat6K(config-vlan)#exit
Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport
Cat6K(config-if)#switchport mode access
Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut
!--- Assigns the port connected to the RADIUS server to
VLAN 10. !--- Note:- All the active access ports are in
VLAN 1 by default.

Cat6K(config-if)#exit
Cat6K(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat6K(config)#interface
range fastEthernet3/2-48
Cat6K(config-if-range)#switchport
Cat6K(config-if-range)#switchport mode access
Cat6K(config-if-range)#dot1x port-control auto
Cat6K(config-if-range)#no shut
!--- Enables 802.1x on all the FastEthernet interfaces.
Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model
!--- Enables AAA. Cat6K(config)#aaa authentication dot1x
default group radius
!--- Method list should be default. Otherwise dot1x does
not work. Cat6K(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS. Cat6K(config)#radius-server host
172.16.1.1
!--- Sets the IP address of the RADIUS server.
Cat6K(config)#radius-server key cisco
!--- The key must match the key used on the RADIUS
server. Cat6K(config)#interface vlan 10
Cat6K(config-if)#ip address 172.16.1.2 255.255.255.0
Cat6K(config-if)#no shut
!--- This is used as the gateway address in RADIUS
```

```
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 2.
Cat6K(config-if)#interface vlan 3
Cat6K(config-if)#ip address 172.16.3.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 3.
Cat6K(config-if)#exit
Cat6K(config)#ip dhcp pool vlan2_clients
Cat6K(dhcp-config)#network 172.16.2.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.2.1
!--- This pool assigns ip address for clients in VLAN 2.
Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1
!--- This pool assigns ip address for clients in VLAN 3.
Cat6K(dhcp-config)#exit
Cat6K(config)#ip dhcp excluded-address 172.16.2.1
Cat6K(config)#ip dhcp excluded-address 172.16.3.1
Cat6K(config-if)#end
Cat6K#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------
-----------------------
1    default                           active    Fa3/2,
Fa3/3, Fa3/4, Fa3/5
                                                 Fa3/6,
Fa3/7, Fa3/8, Fa3/9
                                                 Fa3/10,
Fa3/11, Fa3/12, Fa3/13
                                                 Fa3/14,
Fa3/15, Fa3/16, Fa3/17
                                                 Fa3/18,
Fa3/19, Fa3/20, Fa3/21
                                                 Fa3/22,
Fa3/23, Fa3/24, Fa3/25
                                                 Fa3/26,
Fa3/27, Fa3/28, Fa3/29
                                                 Fa3/30,
Fa3/31, Fa3/32, Fa3/33
                                                 Fa3/34,
Fa3/35, Fa3/36, Fa3/37
                                                 Fa3/38,
Fa3/39, Fa3/40, Fa3/41
                                                 Fa3/42,
Fa3/43, Fa3/44, Fa3/45
                                                 Fa3/46,
Fa3/47, Fa3/48
2    VLAN2                             active
3    VLAN3                             active
10   RADIUS_SERVER                     active    Fa3/1
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
!--- Output suppressed. !--- All active ports are in
VLAN 1 (except 3/1) before authentication.
```

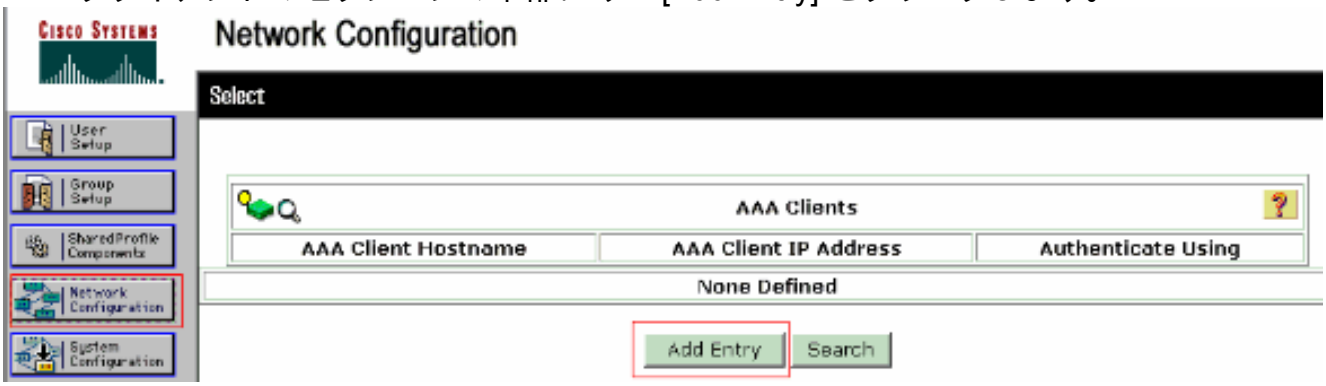
注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセス

できない場合がありますことをご了承ください。

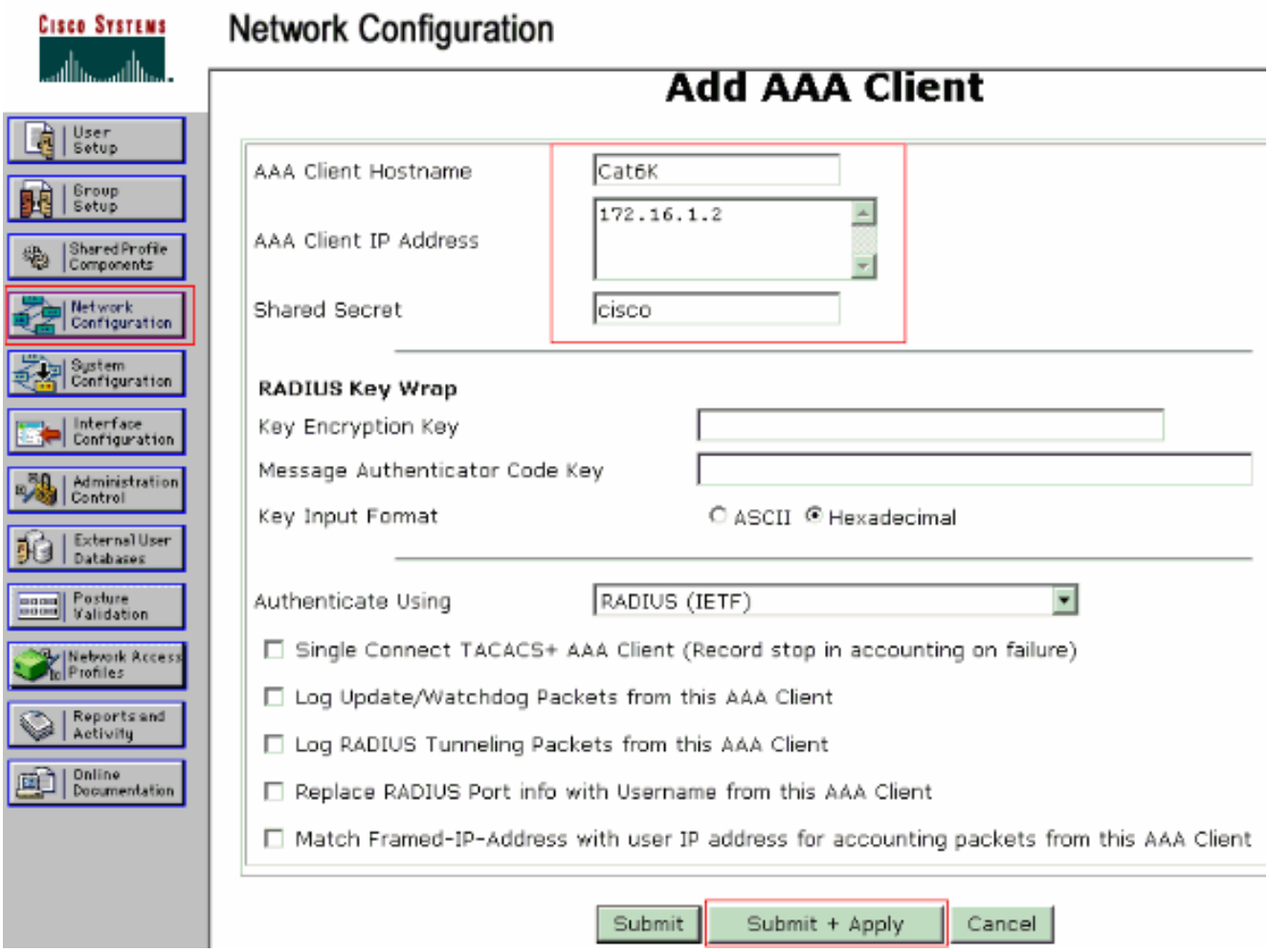
RADIUS サーバの設定

RADIUSサーバには172.16.1.1/24のスタティックIPアドレスが設定されています。AAAクライアント用にRADIUSサーバを設定するには、次の手順を実行します。

1. AAA クライアントを設定するには、ACS 管理ウィンドウで **Network Configuration** をクリックします。
2. AAA クライアントのセクションの下部にある [Add Entry] をクリックします。



3. 次のように、AAA クライアント ホスト名、IP アドレス、共有秘密鍵、および認証タイプを設定します。AAA クライアント ホスト名 = スイッチ ホスト名（**Cat6K**）AAA クライアントの IP アドレス = スイッチの管理インターフェイスの IP アドレス（**172.16.1.2**）共有秘密鍵 = スイッチで設定されている Radius キー（**cisco**）Authenticate Using = **RADIUS IETF注：正しく**操作するには、AAAクライアントとACSで共有秘密キーが同一である必要があります。キーの大文字と小文字は区別されます。
4. これらの変更を有効にするには、次の例に示すように **Submit + Apply** をクリックします。

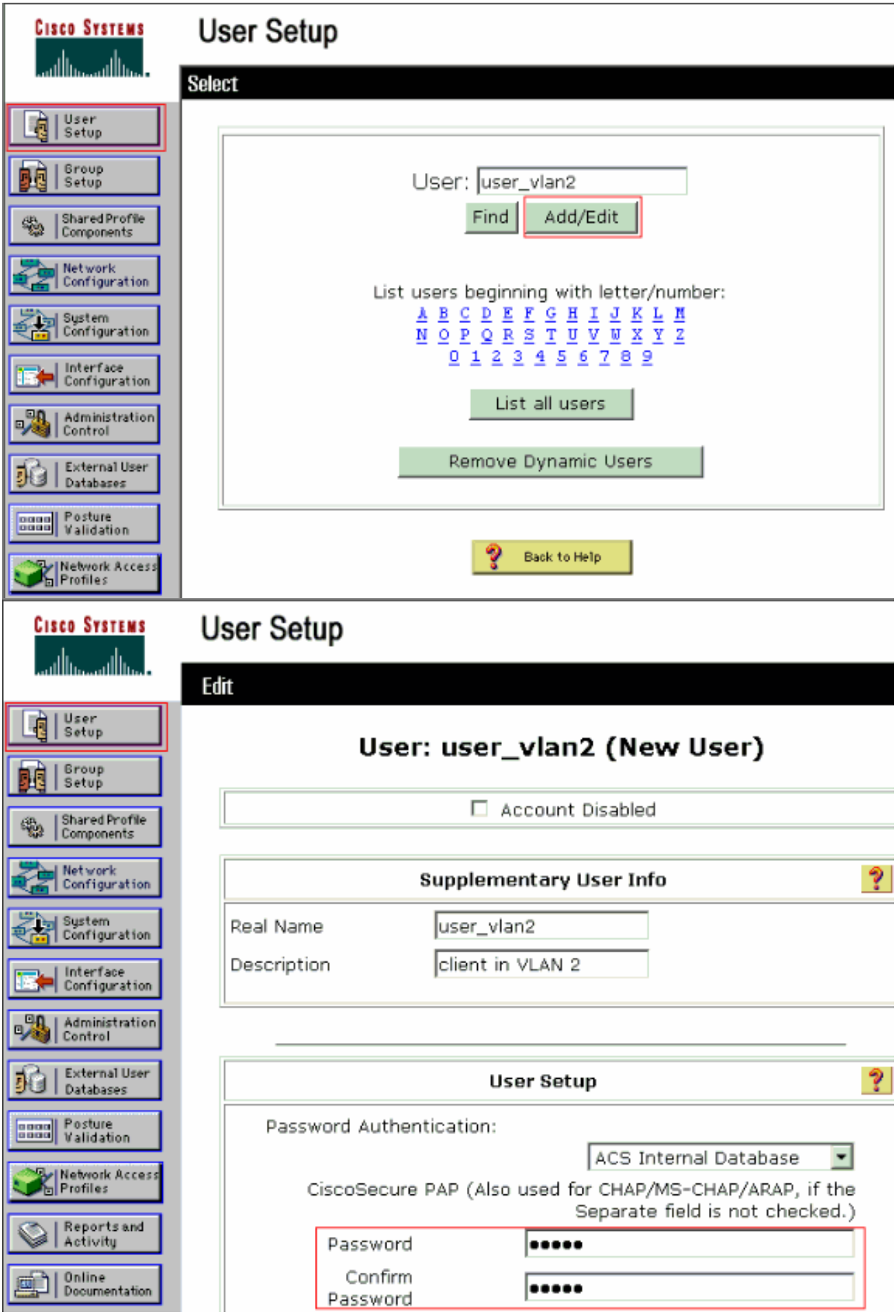


認証、VLAN、およびIPアドレス割り当てのためにRADIUSサーバを設定するには、次の手順を実行します。

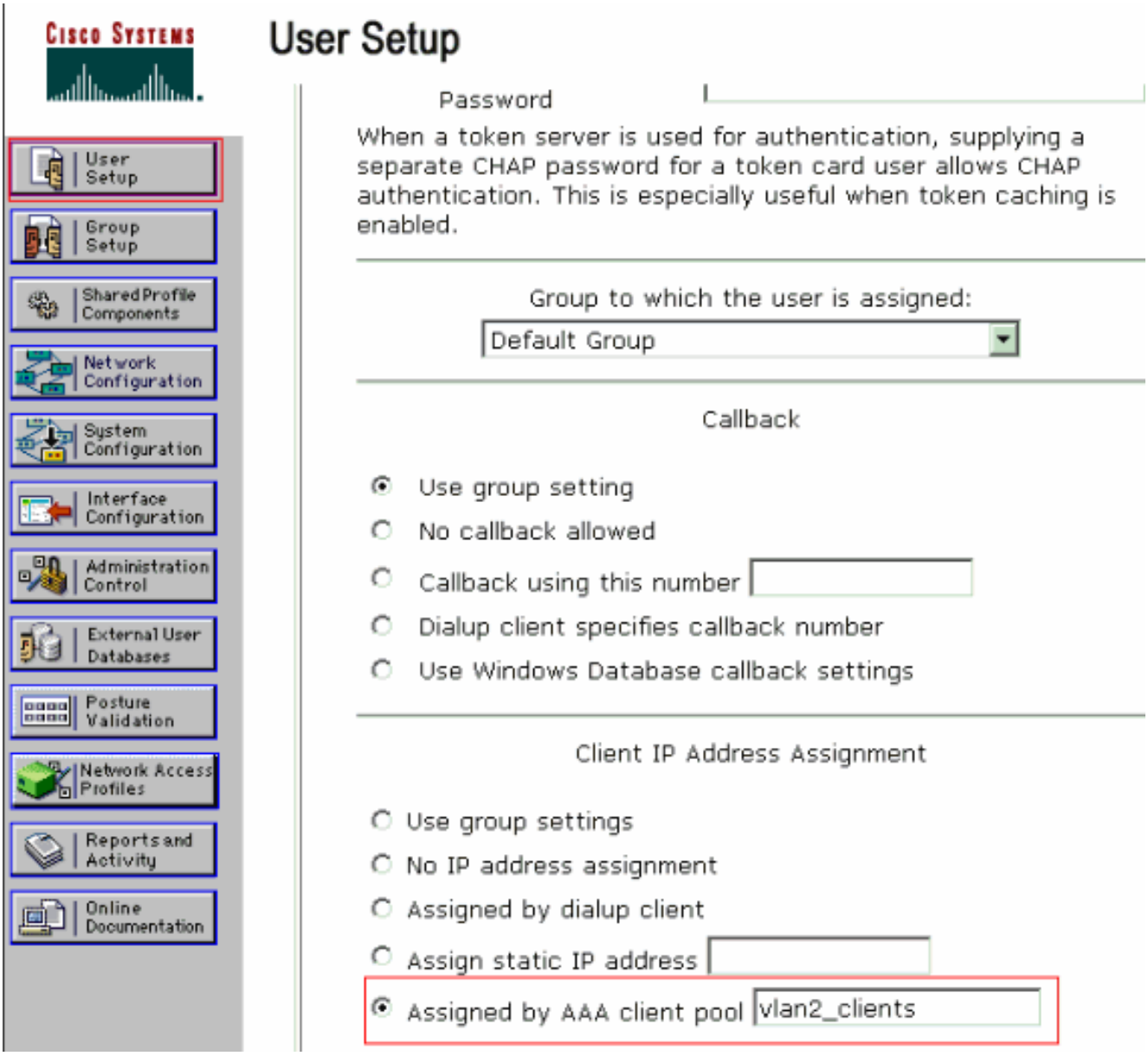
VLAN 2に接続するクライアントとVLAN 3に接続するクライアントに対して、2つのユーザ名を個別に作成する必要があります。ここでは、VLAN 2に接続するクライアント用のユーザ**user_vlan2**と、VLAN 3に接続するクライアント用用**user_vlan3が作成されます。**

注：ここでは、VLAN 2のみに接続するクライアントのユーザ設定を示します。VLAN 3に接続するユーザについても、同じ手順に従います。

1. ユーザを追加および設定するには、[User Setup]をクリックし、ユーザ名とパスワードを定義します。

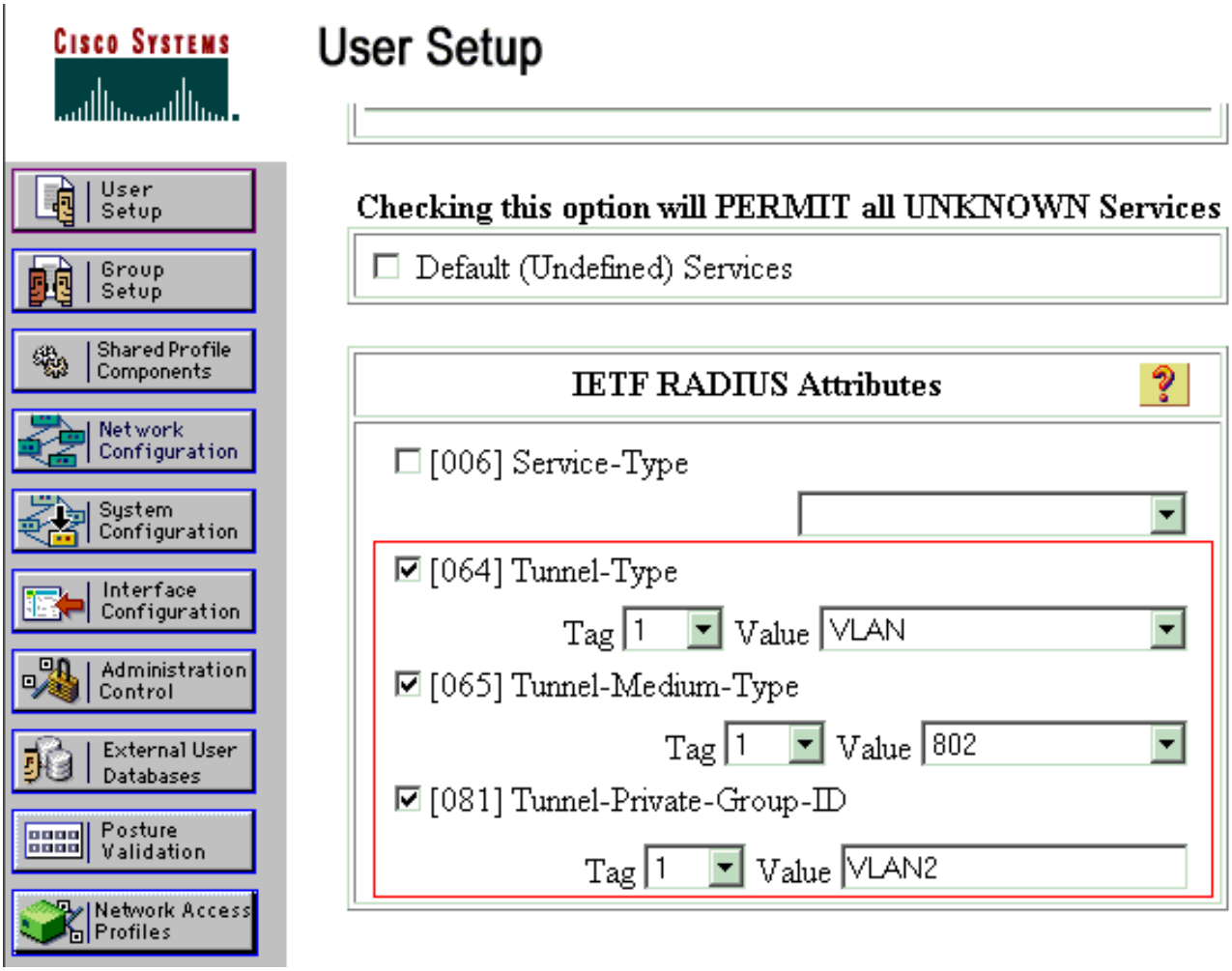


2. **Assigned by AAA client pool** としてクライアント IP アドレス割り当てを定義します。VLAN 2 クライアントのスイッチ上で設定された IP アドレス プールの名前を入力します。



注：このオプションを選択して、AAAクライアントのIPプール名を入力します。このユーザがAAAクライアントに設定されたIPアドレスプールによって割り当てられたIPアドレスを持っている場合にのみ使用します。

3. Internet Engineering Task Force（IETF）の属性 64 および 65 を定義します。この例のように、値のタグには 1 を設定してください。Catalyst では 1 以外のタグは無視されます。ユーザを特定の VLAN に割り当てるには、アトリビュート **81** で、対応する VLAN *名*または VLAN *番号*を指定します。**注：VLAN**名を使用する場合は、スイッチで設定されている名前とまったく同じでなければなりません。



注： これらのIETF属性の詳細については、RFC 2868:RADIUS Attributes for Tunnel Protocol Support』を参照してください。**注：ACSサーバ**の初期設定では、IETF RADIUS属性がユーザ設定で表示されない場合**があります**。ユーザ設定の画面で IETF アトリビュートを有効にするには、**Interface configuration > RADIUS (IETF)** の順にクリックします。 次に、[User and Group] 列で属性 64、65、および 81 にチェックを付けます。**注：**IETF属性**81**を定義せず、ポートがアクセスモードのスイッチポートである場合は、クライアントはポートのアクセスVLANに割り当てられます。ダイナミックVLAN割り当て属性**81を定義して**、ポートがアクセスモードのスイッチポートである場合は、スイッチで**aaa authorization network default group radiusコマンドを発行する必要があ**ります。このコマンドによって、ポートが RADIUS サーバから提供される VLAN に割り当てられます。それ以外の場合、802.1xはユーザの認証後にポートを**AUTHORIZED**状態に移行します。ただし、ポートはポートのデフォルトVLAN内にあり、接続が失敗する可能性があります。属性**81**を定義しているが、ポートをルーテッドポートとして設定している場合、アクセス拒否が発生します。次のエラー メッセージが表示されます。

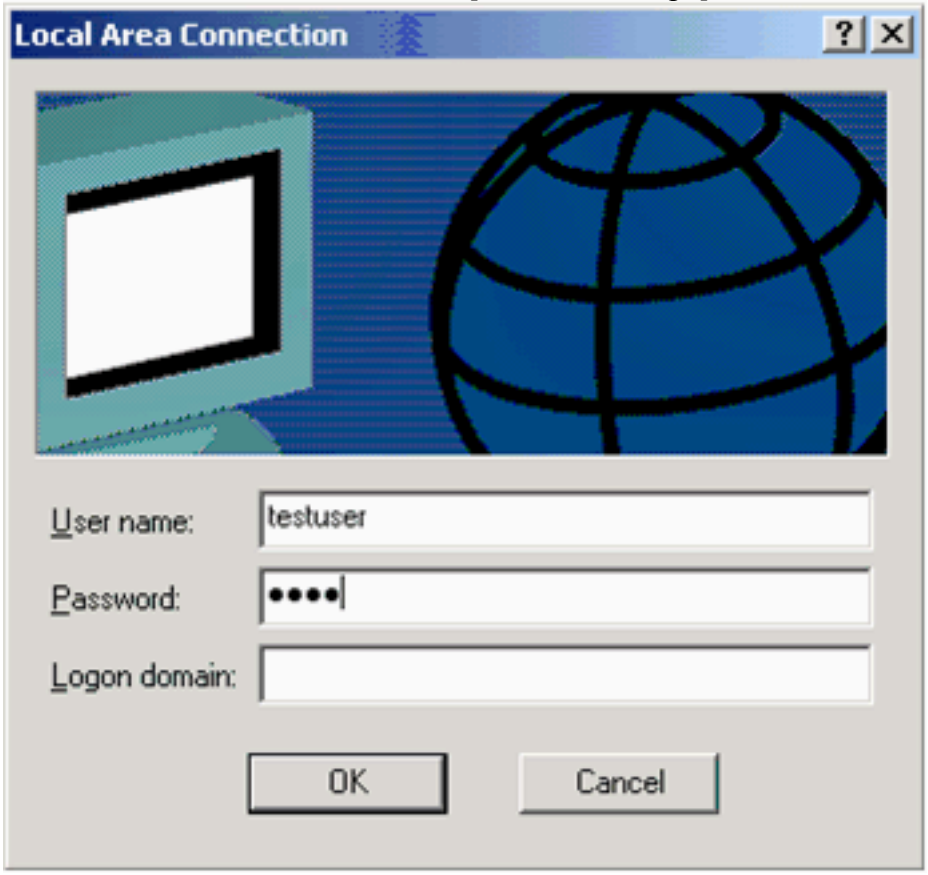
```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
VLAN cannot be assigned.
```

802.1x 認証を使用するための PC クライアントの設定

この設定例は、Microsoft Windows XP の Extensible Authentication Protocol（EAP）over LAN（EAPOL）クライアント固有のものです。

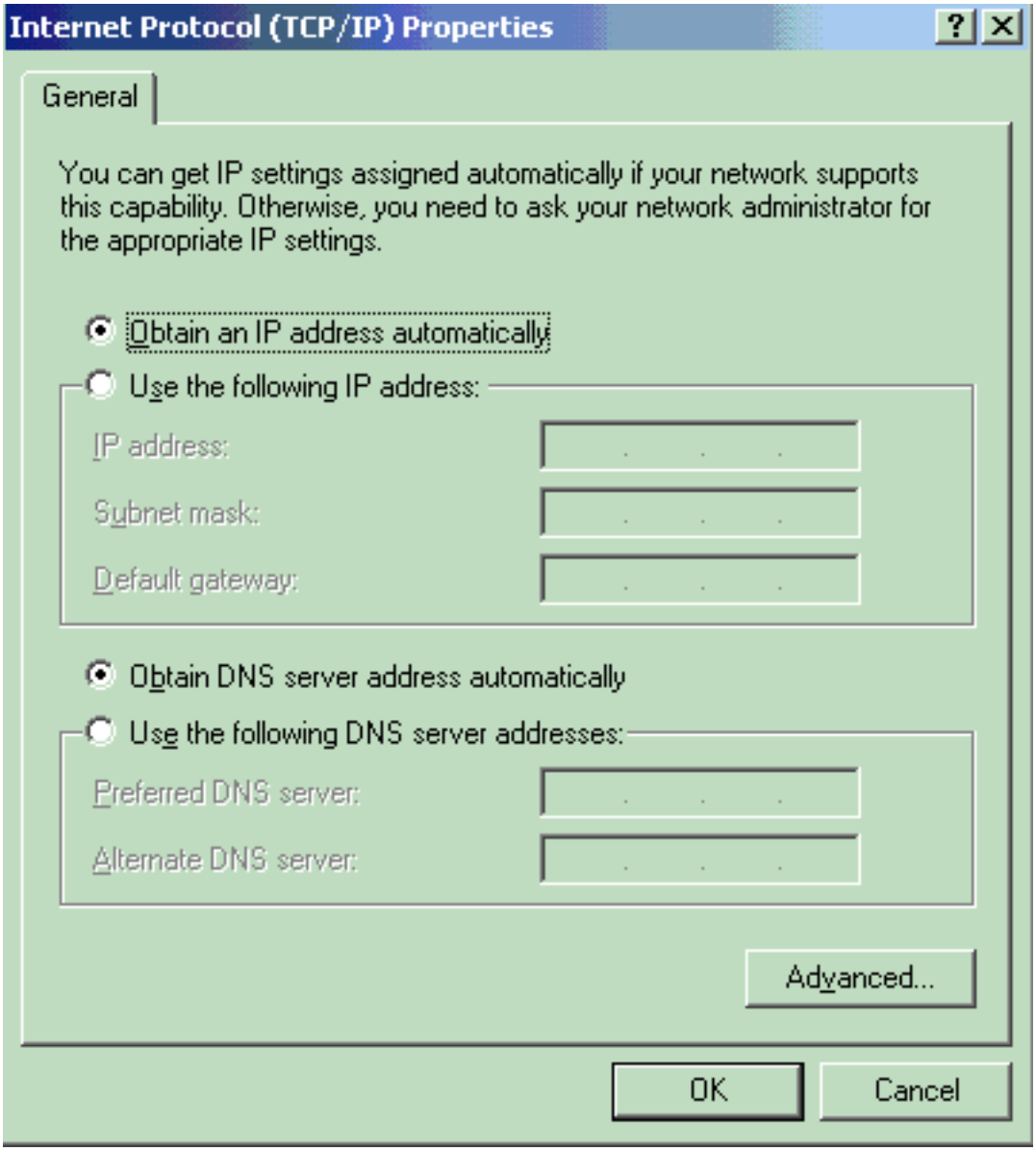
1. **[スタート] > [コントロールパネル] > [ネットワーク接続]** の順にクリックし、**[ローカルエリア接続]** を右クリックして **[プロパティ]** を選択します。

2. General タブで、**Show icon in notification area when connected** にチェックを付けます。
3. [Authentication] タブで、[**Enable IEEE 802.1x authentication for this network**] にチェックを付けます。
4. 次の例のように、EAP の種類に [**MD5-Challenge**] を選択します。



DHCPサーバからIPアドレスを取得するようにクライアントを設定するには、次の手順を実行します。

1. **[スタート] > [コントロールパネル] > [ネットワーク接続]** の順にクリックし、[**ローカルエリア接続**] を右クリックして [**プロパティ**] を選択します。
2. [General] タブで、**[Internet Protocol (TCP/IP)]** をクリックし、**[Properties]**をクリックします。
3. [Obtain an IP address automatically] を選択します。



確認

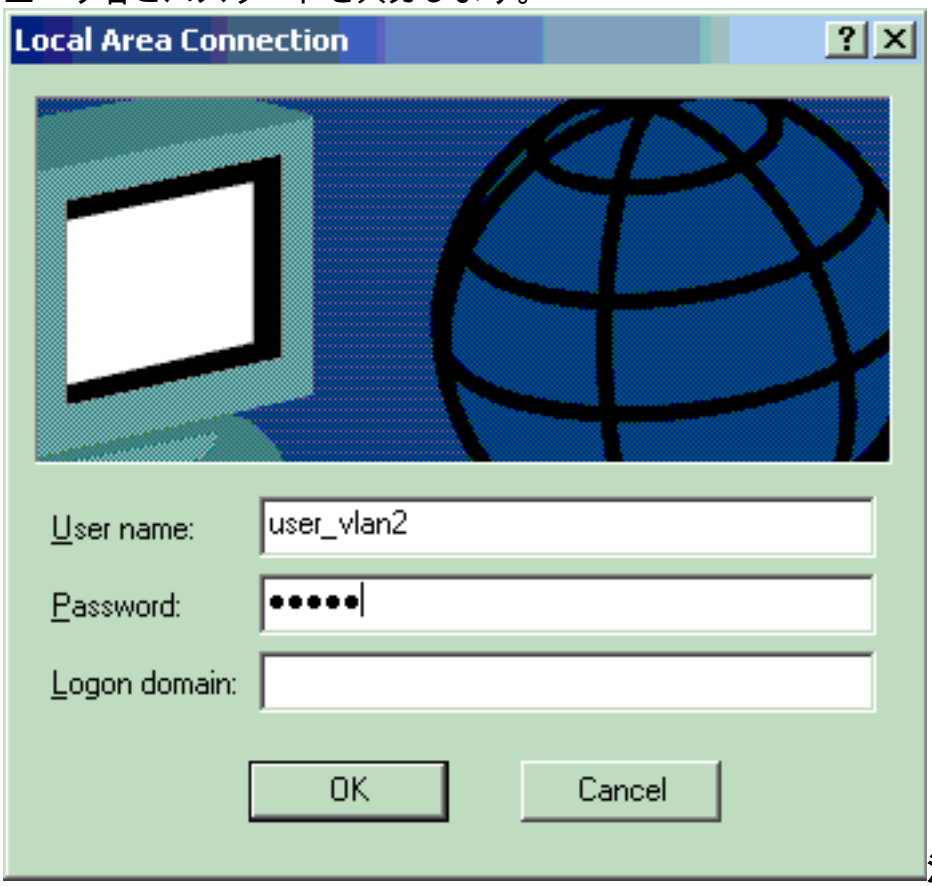
PC クライアント

正しく設定が行われると、PC クライアントにポップアップが表示され、ユーザ名とパスワードの入力をユーザに要求します。

1. 次の例で示すプロンプトをクリックします。

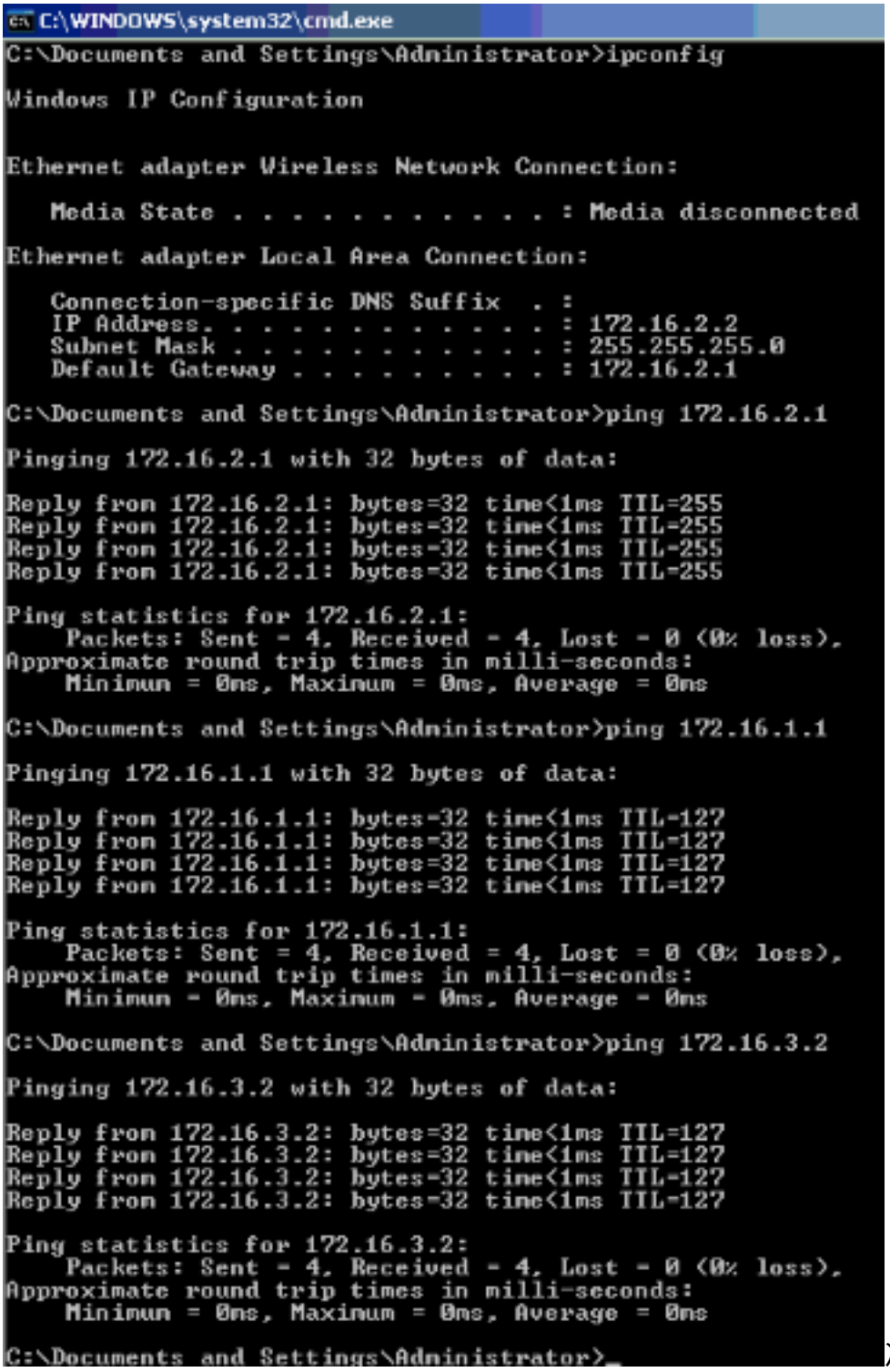
ユーザ名とパスワードを入力するウィンドウが表示されます。

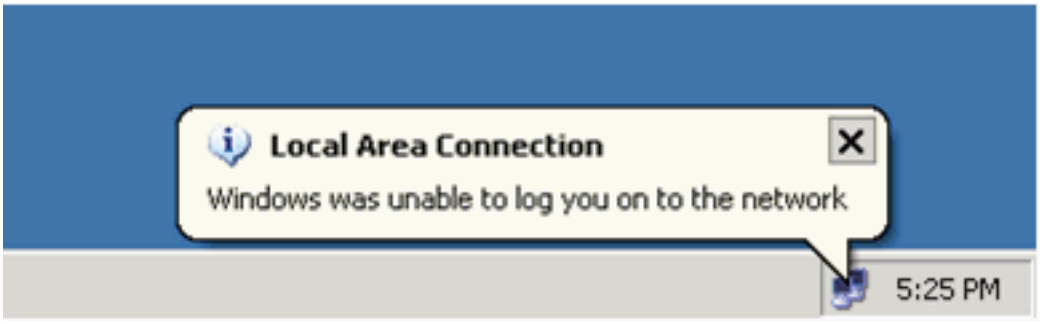
2. ユーザ名とパスワードを入力します。



注：PC 1と2でVLAN 2ユーザクレデンシャルを入力し、PC 3と4でVLAN 3ユーザクレデンシャルを入力します。

3. エラー メッセージが表示されなければ、ネットワーク リソースにアクセスしたり、**ping** を発行したりするなど、通常の方法で接続を確認します。次の出力はPC 1からの出力で、PC 4へのping**が成功**したことを示します。


次のエラーが表示された場合は、ユーザ名とパスワードが正しく入力されているかどうかを確認します。



Catalyst 6500

パスワードとユーザ名が正しく入力されている場合は、スイッチの 802.1x ポートの状態を確認し

ます。

1. AUTHORIZED を示すポート状態を探します。

```
Cat6K#show dot1x

Sysauthcontrol                  = Enabled
Dot1x Protocol Version          = 1
Dot1x Oper Controlled Directions  = Both
Dot1x Admin Controlled Directions = Both


Cat6K#show dot1x interface fastEthernet 3/2
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Enabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds

Cat6K#show dot1x interface fastEthernet 3/4
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Enabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds

Cat6K#show dot1x interface fastEthernet 3/1
Default Dot1x Configuration Exists for this interface FastEthernet3/1
AuthSM State      = FORCE AUTHORIZED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Disabled
PortControl       = Force Authorized
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
```

認証に成功した後、VLAN ステータスを確認します。

```
Cat6K#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa3/6, Fa3/7, Fa3/8, Fa3/9,
                                                Fa3/10, Fa3/11, Fa3/12, Fa3/13,
                                                Fa3/14, Fa3/15, Fa3/16, Fa3/17,
                                                Fa3/18, Fa3/19, Fa3/20, Fa3/21,
                                                Fa3/22, Fa3/23, Fa3/24, Fa3/25,
```

```
                                                Fa3/26, Fa3/27, Fa3/28, Fa3/29,
                                                Fa3/30, Fa3/31, Fa3/32, Fa3/33,
                                                Fa3/34, Fa3/35, Fa3/36, Fa3/37,
                                                Fa3/38, Fa3/39, Fa3/40, Fa3/41,
                                                Fa3/42, Fa3/43, Fa3/44, Fa3/45,
                                                Fa3/46, Fa3/47, Fa3/48
2    VLAN2                          active     Fa3/2, Fa3/3
3    VLAN3                          active     Fa3/4, Fa3/5
10   RADIUS_SERVER                  active     Fa3/1
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default                act/unsup
1005 trnet-default                  act/unsup
!--- Output suppressed.
```

2. 認証に成功した後のDHCPバインディングステータスを確認します。

```
Router#show ip dhcp binding
IP address       Hardware address        Lease expiration        Type
172.16.2.2       0100.1636.3333.9c       Mar 04 2007 06:35 AM    Automatic
172.16.2.3       0100.166F.3CA3.42       Mar 04 2007 06:43 AM    Automatic
172.16.3.2       0100.145e.945f.99       Mar 04 2007 06:50 AM    Automatic
172.16.3.3       0100.1185.8D9A.F9       Mar 04 2007 06:57 AM    Automatic
```

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

トラブルシュート

トラブルシューティングを行うには、次の**debug**コマンドの出力を収集します。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug dot1x events**:dot1x eventsフラグで保護されたprint文のデバッグを有効にします。

```
Cat6K#debug dot1x events
Dot1x events debugging is on
Cat6K#
!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: dot1x-ev:Got a Request from SP to
send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0
00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 00:13:36: dot1x-
ev:The Interface on which we got this AAA Request
   is FastEthernet3/2
00:13:36: dot1x-ev:MAC Address is 0016.3633.339c
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 6
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15
00:13:36: dot1x-ev:Found a process thats already handling therequest for
    this id 12
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 31
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16
00:13:36: dot1x-ev:Found a process thats already handling therequest for
   this id 13
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:13:36: dot1x-ev:Vlan name = VLAN2
00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM -
```

```
   id 16 EAP pkt len = 4
00:13:37: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
Cat6K#
!--- Debug output for PC 3 connected to Fa3/4. 00:19:58: dot1x-ev:Got a Request from SP to
send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0
00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 00:19:58: dot1x-
ev:The Interface on which we got this AAA
   Request is FastEthernet3/4
00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 6
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 10
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 31
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 11
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:19:58: dot1x-ev:Vlan name = 3
00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4
00:19:58: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
```

- **debug radius**:RADIUSに関連する情報を表示します。

```
Cat6K#debug radius
Radius protocol debugging is on
Cat6K#
!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: RADIUS: ustruct sharecount=1
00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-
login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit
FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6
AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36:
Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18
CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79
00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80
18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-
login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS:
Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius
packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18
172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80
18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104
00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80
18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-
login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS:
Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius
packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19
172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80
18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124
```

```
00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8
01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFE 00:13:36:
Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18
11A7DD44 00:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K# Cat6K# !--- Debug
output for PC 3 connected to Fa3/4. 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS:
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11
172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute
61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58:
Attribute 79 17 0201000F 00:19:58: Attribute 80 18 0001AC52 00:19:58: RADIUS: Received from
id 11 172.16.1.1:1812, Access-Challenge, len 79 00:19:58: Attribute 79 8 010B0006 00:19:58:
Attribute 24 33 43495343 00:19:58: Attribute 80 18 23B9C9E7 00:19:58: RADIUS: EAP-login:
length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58:
RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812, Access-Request,
len 109 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80 18 F4C8832E 00:19:58: RADIUS:
Received from id 12 172.16.1.1:1812, Access-Challenge, len 104 00:19:58: Attribute 79 33
010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 45472A93 00:19:58:
RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-login: got challenge from
radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812, Access-Request,
len 135 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80 18 37011E8F 00:19:58: RADIUS:
Received from id 13 172.16.1.1:1812, Access-Accept, len 120 00:19:58: Attribute 64 6
0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4 0133580F 00:19:58:
Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58: Attribute 79 6 030C0004
00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18 F5520A95 00:19:58: RADIUS: EAP-
login: length of eap packet = 4 Cat6K#
```

関連情報

- CatOS ソフトウェアが稼動する Catalyst 6500/6000 での IEEE 802.1x 認証の設定例
- Cisco Catalyst スイッチ環境で Windows NT/2000 Server 用 Cisco Secure ACS を導入する際のガイドライン
- RFC 2868:RADIUS Attributes for Tunnel Protocol Support
- IEEE 802.1Xポートベース認証の設定
- LAN 製品に関するサポート ページ
- LAN スイッチング テクノロジーに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems